

DRAFT

HST VISION 2000

RISK MANAGEMENT PLAN

A. J. Gainsborough, Manager
HST VISION 2000

A.C.Merwarth, Manager
HST Operations & Ground Systems Project

January, 1997

Table of Contents

Section 1.0 Introduction

1.1 Purpose

1.2 Scope

1.3 Authority

Section 2.0 Approach

2.1 Concept

2.2 Definitions

2.3 Risk Abatement Strategy

2.4 Risk Budgeting

Section 3.0 Application

3.1 External Threats

3.2 Risk Abatement

3.3 Functional Level Risk Management

3.4 Guidelines & Requirements

VISION 2000 RISK MANAGEMENT PLAN

1.0 Introduction

1.1 Purpose

The purpose of this Plan is to establish a process and guidelines for reducing the risks associated with the reengineering of HST operations designated as HST VISION 2000. The objectives and implementation approach for VISION 2000 are described in TBD¹. This Plan identifies the critical risks and the means to be employed for avoiding or mitigating it at the systems level. It also establishes the risk abatement guidelines and requirements for the Product Development Teams (PDT) responsible for implementing the separate functional areas comprising VISION 2000.

1.2 Scope

This Plan focuses principally on the development of the VISION 2000 Control Center System (CCS) and the SSM Flight Software (SSM) development for the 486 on-board computer. The other functional areas comprising VISION 2000 - Science Data Processing (SDP), Planning & Scheduling (P&S), and Payload Flight Software (PFS) - employ an evolutionary development approach involving enhancements to existing, proven systems, and, as such, have minimal risk associated with them. The interactions and integration of all these functional areas are covered, however, within the scope of this Plan.

1.3 Authority

The Manager for VISION 2000 is responsible for the preparation and maintenance of the Plan. Once approved, the Plan is controlled at Level IIIA and remains in effect for the duration of the VISION 2000 implementation. Subsidiary Risk Management Plans for the individual PDTs must be in compliance with this Plan and are to be approved by the VISION 2000 Manager.

¹ HST VISION 2000 Commitment Document?

2.0 Approach

2.1 Concept

Risk management is to be accomplished by:

- a. Identifying potential environmental threats along with their probability of occurrence and impact on the development objectives.
- b. Establishing up-front risk avoidance and/or mitigation strategies along the lines of contingency plans and risk abatement actions to counter these threats.
- c. Anticipating future and unforeseen risk factors by explicitly defining and employing risk abatement procedures as part of the development process both at the systems level and the functional levels, i.e., Product Development Teams.
- d. Focussing on the higher risk functional areas, the Control Center System and the SSM Flight Software.

In general terms, risk management relies on good information exchange with users, developers, and management having a common understanding of what is required (both functionally and programmatically) and shared responsibility for identifying potential risk factors or threats in a timely fashion at any level within the organization.

2.2 Definitions

Risk is defined as failure to meet any one of these four primary development objectives:

- a. Provide a functional system which fully meets the requirements of the operators and scientists. The capabilities must be both necessary and sufficient for efficient, optimal, and, as importantly, safe operation of the HST. The on-going utilization of HST cannot be jeopardized.
- b. Provide a system which meets high quality standards. The system must be reliable and easily maintained.
- c. Provide the system on schedule and within the allocated resources. Meeting the external schedule drivers associated with future HST servicing missions is mandatory.
- d. Provide a system which dramatically reduces the long term cost of maintenance and operation. This is the principle reason for initiating the VISION 2000 development activity.

Risk factors, often simply called risks, are usually process related causes for development shortfalls or failures. Examples are inadequate tools or expertise, poor requirements definition, inadequate development performance measurements, and careless change or configuration control.

2.3 Risk Abatement Strategy

Threats to meeting objectives are reduced by a development strategy which, in general terms:

- Identifies and provides appropriate skills where needed
- Provides consistent direction & management
- Establishes resource goals and requirement; quantifying project objectives
- Assures that the functional, performance and operational requirements of the system under development are well understood

- Has users validate requirements
- Keeps users involved
- Provides adequate & timely training to developers
- Establishes & tracks performance metrics to anticipate problems
- Establishes & tracks decision checkpoints and delivery events
- Maintains good organizational liaisons to handle interdependencies or linked development schedules

2.4 Risk Budgeting

Normally, risk abatement utilizes the costs and probabilities of occurrence and impact with and without abatement to determine whether to accept the risk. Because of the high visibility of HST and its importance to science and to the Agency, it has been decided that some form of abatement is mandatory for all system level threats against VISION 2000 development objectives. At the PDT level, risk acceptance is permitted with adequate rationale.

3.0 Application

3.1 External Threats

External threats, in general, are not really subject to either control or abatement. Reduction in risk then relies on having contingency approaches or work-arounds or by shielding the project. The principal external threats currently perceived and their probability of occurrence (POC), along with the VISION 2000 counter strategies, are shown in Table 3.1. Item #6 recognizes that the HST has very high visibility and degraded performance or failures are not tolerable. In this case, all risk factors, regardless of probability of occurrence, and to a great extent, impact on the project objectives, must be considered and abated.

Table 3.1

	THREAT	POC	STRATEGY
1	Loss of funding for major development after 2000	H	System release planning & estimated resources required conform to likely budget profile
2	Loss of funding prior to 2000.	M	Prioritization of requirements coupled with adequate end-to-end functionality in early builds to maintain current service level (but decreased future O&M reductions).
3	Loss of expertise when support contract ends before development completion	L	Extend tasks into a new short term contract (CHAMP) with JSC agreement
4	Earlier need date to support SM99	L	Some slack time in 486 S/W development (critical path item) allows minor date movement. Full back-out capability to current control center also possible. Release 2 of CCS capable of full mission support.
5	Mandated Civil Servant	M	Appeal (successful to date) to upper management

	reduction - loss of management expertise		based on need to maintain work force. Synergistic use of CS and contractors in integrated Team approach
6	Conducting an ambitious program in a zero-fault tolerant organization	H	Attention to development process details. Outside Peer Review and frequent internal reviews. Good tracking metrics.
7	Impact of new technology	H	Selecting emerging de facto standards (WEB, JAVA). Maintaining fall-backs, developing pilots (Warehouse), and building early (ATM Networks).

3.2 Risk Abatement

Table 3.2 addresses the approach adopted to avoid or mitigate the risks identified in Section 2.2 associated with the HST VISION 2000 development. In all cases, not meeting the VISION 2000 objective is unacceptable. At the system level, a primary concern is for risk factors, either technical or programmatic, which result in inter-functional subsystem impacts due to subsystem interdependencies. Linked subsystem developments, particularly where there is little slack, can aggravate and compound risk. The two principal mechanisms employed within the VISION 2000 program to achieve risk abatement for interdependent factors are:

1. Open and frequent information exchange by all PDTs through the auspices of the System Architecture Board so that problems can be anticipated early and remedies implemented while maintaining full system perspective.
2. Establishing, maintaining and publicizing a detailed timetable for systems transition explicitly showing all key checkpoints, interdependencies, and relationship to external milestone drivers.

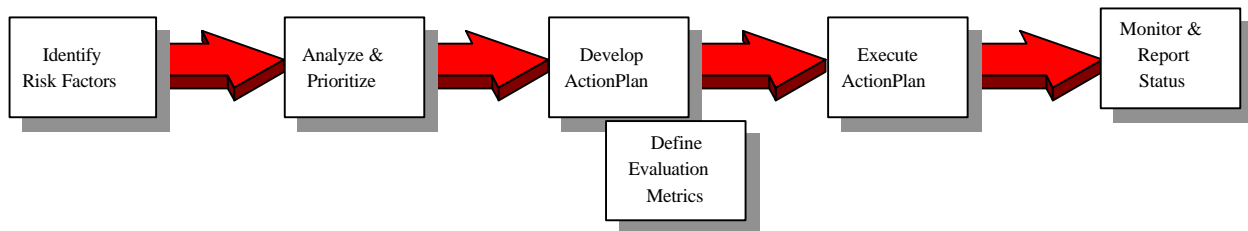
Table 3.2

	RISK	Impact	MITIGATION
1	Not delivering functional capability desired	H	<ul style="list-style-type: none"> • Document & validate requirements vs. current requirements documentation, V2K Operations Concept, and DLPs. • Operators are part of development Teams. • Use a boot-strap verification of the new systems vs. current simulators, truth data & spacecraft (shadow mode)
2	Not providing adequate quality	H	<ul style="list-style-type: none"> • Use Peer Review for process adequacy check. • Periodic internal reviews of results • Verify using boot-strap process • Use of simulators and shadow mode
3	Not meeting schedule	H	<ul style="list-style-type: none"> • Use of top-down transition planning. • Defining key check points. Use of product oriented metrics for status tracking. • Maintaining schedule surveillance at subsystem. level and frequent information exchanges re problems.
4	Not realizing a dramatic cost reduction in O&M	H	<ul style="list-style-type: none"> • Design focused on operational implications. • Careful make-buy trades.

- Use most appropriate S/W methodology.
 - Continual check & update of staffing projections vs. system design.
- 5 Not delivering within allocated resources **L-M**
- Estimating resources required using models & experience (COCOMO allowing for OO).
 - Tracking/reporting status at detailed level.
 - Synergy with other projects (ECS).

3.3 Functional Level Risk Management

The generalized process flow for risk abatement at the subsystem level i.e., within the PDTs, is shown in the following diagram.



The key features or steps involved are as follows:

- Anyone may identify & report a possible risk factor
- Team or Group Leads validate risk factor
- Probability of occurrence & impact are established
- Data are entered into a Risk Management Data Base
- Actions Plans are prepared for higher priority items
- Plan is approved by the Team Lead and PDT Manager
- Plan may call for avoidance, mitigation, transferal, or acceptance of risk
- Single point of contact identified for management of implementation activities specified by Plan
- Team Lead & PDT Manager determine effectiveness
- All risk factors deemed to have interdependent impacts on other functional areas are subject to System Architecture Board control.

3.4 Guidelines & Requirements

The CCS and SSM PDTs may implement their own support systems to accomplish risk management but these essential requirements must be met.

1. A brief Risk Management Plan is to be prepared which describes the adopted process flow.
2. Plan approval is by the PDT Manager with concurrence by the VISION 2000 Manager.
3. A data base of risk factors, along with probability of occurrence and impact severity is to be maintained and kept current by each PDT.

4. The data base shall contain either the risk abatement approach or rationale for accepting the risk factor.
5. Status information regarding the implementation and effectiveness of risk abatement approaches shall be available on the Net.
6. The PDT Manager shall alert the Systems Architecture Board regarding any risk factors which may impact other functional areas or result in compounded risks at the system level.
7. Risk management status shall be presented routinely at all external Peer or internal reviews.

The P&S, SDP and PFS PDTs, because of the evolutionary development approach being employed, are subject to far less risk and continue using their current strategies for project management and control.